CLAIMS

1. A computer-implemented method for creating a cryptographically secure network between at least two access systems, the method comprising a switch system performing the steps of:

associating each of a plurality of access systems with a public key from a private-public key pair associated with said access system;

in response to a request from a first access system to transmit data to a second access system:

authenticating the first access system using the public key associated with the first access system;

forming a first cryptographically secure network connection between the authenticated first access system and the switch system;

accepting data from the authenticated first access system via the first cryptographically secure network connection;

authenticating the second access system using the public key associated with the second access system;

forming a second cryptographically secure network connection between the authenticated second access system and the switch system; and

transmitting the data to the authenticated second access system via the second cryptographically secure network connection.

2. The method of claim 1 wherein the switch system issues to an access system the access system's private-pubic key pair.

3. The method of claim 1 wherein the switch system comprises a plurality of nodes securely networked together.

4. The method of claim 2 wherein the first and second access systems connect to the switch system via different nodes.

5. The method of claim 1 further comprising the switch system performing the step of:

using a switch system private key, in conjunction with an access system using a corresponding switch system public key, to authenticate the switch system to the access system.

6. The method of claim 1 wherein the first and second cryptographically secure connections are each implemented by encrypting the data at a layer selected from the group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnection reference model.

7. The method of claim 6 wherein the first and second cryptographically secure network connections are each formed using at least one encryption key from a group comprising a symmetric key, an asymmetric key, and a symmetric session key encrypted with an asymmetric key.

8. The method of claim 1 wherein the data is encrypted with at least one encryption key for which the switch system does not have access to the encryption key's corresponding decryption key.

9. The method of claim 1 wherein the data comprises at least one from the group comprising:

a digest of at least a portion of the data; and

a digital signature of the first access system.

10. The method of claim 1 further comprising the switch system performing the step of storing at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature.

11. The method of claim 10 further comprising the switch system performing the step of time-stamping at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature of the first access system.

12. The method of claim 1 wherein the switch system interfaces with an application which utilizes the data exchanged between the first and second access systems.

13. The method of claim 1 wherein at least one of the first and second access systems connects to the switch system via an application proxy.

14. The method of claim 13 wherein the application proxy processes data initiated from an access system and data intended for the access system based upon predefined policies.

15. The method of claim 14 wherein the policies for the application proxy are set by the access system.

16. A switch system for establishing a secure network connection between at least two access systems, the switch system comprising:

at least one node comprising:

a key module for associating each access system with a public key from a private-public key pair associated with said access system;

an authentication module, coupled to the key manager module, for using an access system's public key, in conjunction with the access system using its private key, to authenticate the access system; and

a secure network module, coupled to the authentication module, for establishing a cryptographically secure network connection between the switch system and an authenticated access system, whereby data is received from a first access system via a first secure connection and transmitted to a second access system via a second secure connection.

17. The system of claim 16 wherein the key module is further adapted to perform the step of:

issuing a private-public key pair to an access system.

18. The system of claim 16 wherein the authentication module is further adapted to perform the step of:

using a switch system private key, in conjunction with an access system using a corresponding switch system public key, to authenticate the switch system to the access system.

19. The system of claim 16 wherein the cryptographically secure network connection is implemented by encrypting the data at a layer selected from the group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnection reference model.

20. The system of claim 19 wherein the cryptographically secure network connections are formed using at least one encryption key from the group comprising a symmetric key, an asymmetric key, and a symmetric session key encrypted with an asymmetric key.

21. The system of claim 16 wherein the data is encrypted with at least one encryption key for which the switch system does not have access to the encryption key's corresponding decryption key.

22. The system of claim 16 wherein the node further comprises:

a computer-readable medium for storing at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature of an access system.

23. The system of claim 16 wherein the node further comprises:

a tracking module for time-stamping and storing at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature of an access system.

24. The system of claim 16 wherein the node further comprises:

an interface module for interfacing with a network application to provide a service in conjunction with the data transferred via the switch system.

25. The system of claim 16 further comprising a plurality of nodes securely networked together.

26. The system of claim 16 further comprising:

an application proxy for processing the data initiated from an access system and data intended for the access system based upon predefined policies.

27. An access system for establishing a cryptographically secure connection to a switch system, the access system comprising:

a key module for accessing a private-public key pair of a user of the access system;

an authentication module, coupled to the key module, for authenticating to the switch system using the private-public key pair; and

a secure network connection module, coupled to the authentication module, for establishing a cryptographically secure connection between the switch system and the access system, wherein data is transmitted to and received data from the switch system via the cryptographically secure connection.

28. The system of claim 27 wherein the key module is further adapted to perform the step of:

generating a private-public key pair for the user.

29. The system of claim 27 wherein the authentication module is further adapted to perform the step of:

using a switch system public key, in conjunction with the switch system using a corresponding switch system private key, to authenticate the switch system to the access system.

30. The system of claim 27 wherein the cryptographically secure network connection is implemented by encrypting the data at a layer selected from the group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnect reference model.

31. The system of claim 30 wherein the cryptographically secure network connections are formed using at least one encryption key from the group comprising a symmetric key, an asymmetric key, and a symmetric session key encrypted with an asymmetric key.

32. The system of claim 27 wherein the data is encrypted with at least one encryption key for which the switch system does not have access to the encryption key's corresponding decryption key.

33. The system of claim 27 wherein the secure network connection module is further adapted for generating at least one of the group comprising a digest of at least a portion of the data and a digital signature of the access system.

34. The system of claim 27 wherein the access system is implemented in a secure-network-connection application proxy.

35. The system of claim 34 wherein the secure-network-connection application proxy is accessed by more than one client system.

36. The system of claim 34 wherein the secure-network-connection application proxy processes data initiated from a client system and data intended for the client system based upon predefined policies.

37. The system of claim 27 wherein the access system is implemented in a secure-network-connection enabled application.

38. The system of claim 27 wherein the access system is implemented through a set of application program interfaces.

39. In a computer-readable medium, a computer program product for creating a cryptographically secure network between at least two access systems, the computer-readable medium comprising program code adapted to perform the steps of:

associating each of a plurality of access systems with a public key from a private-public key pair associated with said access system;

in response to a request from a first access system to transmit data to a second access system:

authenticating the first access system using the public key associated with the first access system;

forming a first cryptographically secure network connection between the authenticated first access system and the switch system;

accepting data from the authenticated first access system via the first cryptographically secure network connection;

authenticating the second access system using the public key associated with the second access system;

forming a second cryptographically secure network connection between the authenticated second access system and the switch system; and

transmitting the data to the authenticated second access system via the second cryptographically secure network connection.

40. The computer readable medium of claim 39 wherein the switch system issues to an access system the access system's private-pubic key pair.

41. The computer readable medium of claim 39 wherein the switch system comprises a plurality of nodes securely networked together.

42. The computer readable medium of claim 41 wherein the first and second access systems connect to the switch system via different nodes.

43. The computer readable medium of claim 39 further comprising program code adapted to perform the step of:

using a switch system private key, in conjunction with an access system using a corresponding switch system public key, to authenticate the switch system to the access system.

44. The computer readable medium of claim 39 wherein the first and second cryptographically secure connections are each implemented by encrypting the data at a layer selected from the group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnection reference model.

45. The computer readable medium of claim 44 wherein the first and second cryptographically secure network connections are each formed using at least one encryption key from the group comprising a symmetric key, an asymmetric key, and a symmetric session key encrypted with an asymmetric key.

46. The computer readable medium of claim 39 wherein the data is encrypted with at least one encryption key for which the switch system does not have access to the encryption key's corresponding decryption key.

47. The computer readable medium of claim 39 wherein the data further comprises at least one from the group comprising:

a digest of at least a portion of the data; and

a digital signature of the first access system.

48. The computer readable medium of claim 39 further comprising program code adapted to perform the step of:

storing at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature.

49. The computer readable medium of claim 48 further comprising program code adapted to perform the step of:

time-stamping at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature of the first access system.

50. The computer readable medium of claim 39 wherein the switch system interfaces with an application which utilizes the data exchanged between the first and second access systems.

51. The computer readable medium of claim 39 wherein at least one of the first and second access systems connects to the switch system via an application proxy.

52. The computer readable medium of claim 51 wherein the application proxy processes data initiated from an access system and data intended for the access system based upon predefined policies.

53. The computer readable medium of claim 52 wherein the policies for the application proxy are set by the access system.